Maryland

DEPARTMENT OF HEALTH
Dennis R. Schrader, Secretary
DEPARTMENT OF INFORMATION TECHNOLOGY
Michael G. Leahy, Secretary

Remarks by the Maryland Department of Information Technology and Maryland Department of Health before the Senate Education, Health, and Environmental Affairs and House Health and Government Operations Committees.

Thursday, January 13, 2022

Presenters:

Chip Stewart, State Chief Information Security Officer, Department of Information Technology (DoIT)

Lance Schine, Deputy Secretary and State Chief Technology Officer, DoIT

Atif Chaudhry, Deputy Secretary (Operations), Maryland Department of Health (MDH)

Dennis R. Schrader, Secretary, MDH

Chief Information Security Officer Chip Stewart

Good afternoon. My name is Chip Stewart, Chief Information Security Officer for the State of Maryland – a position I have held since 2019. Before that, I worked with the State as a contractor supporting the Department of Information Technology and the Department of Budget and Management when the agency oversaw the networkMaryland program. My involvement in supporting the State with its technology and security initiatives goes back to 2004.

As you are aware, the Maryland Department of Health experienced a service disruption on December 4th as a result of a network security incident. We have provided a number of briefings to legislative and committee leaders, the Comptroller, the Treasurer, the Attorney General, and the congressional delegation.

While the investigation is ongoing – and is occurring on a parallel track to our restoration efforts – we can confirm this much today: this was, in fact, a ransomware attack. We have paid no extortion demand, and my recommendation—after consulting with our vendors and law enforcement—is we do not pay any such demand.

It would be premature and potentially damaging to the investigation and to the security of our systems to disclose additional details. At this time, we also cannot speak to the motive or motives of the threat actor. Both law enforcement and cybersecurity authorities have

observed that health and hospital systems are increasingly being targeted by malicious actors during the pandemic.

Again, we are still very much in the midst of an active investigation, so we are limited in what information we can share – and I thank you for recognizing and appreciating that. We have evaluated the risk related to sharing additional details with you and the public today and feel that this disclosure represents a balance between transparency, security, and maintaining the integrity of the investigation. I also want to be clear that I am not able to speak to the specific tools and capabilities of the Maryland Department of Health's IT and Cybersecurity teams for the obvious reason that we cannot disclose such sensitive information that could be used to harm the MDH network or the citizens of Maryland.

I also want to address the offer to hold an executive session to discuss this incident further. We have been informed by our internal legal counsel that, in this case, an executive session would not provide the ongoing confidentiality needed to protect sensitive information about the investigation and our IT security systems. As cybersecurity threats are ever-present, we have a duty to Marylanders to protect information that could be used by threat actors to target the state in the future.

I can, however, speak in some depth about incident response and detection, including how the MDH IT and cybersecurity teams first identified the attack, how our incident response team kicked into gear, and our ongoing restoration efforts.

During the early morning hours of Saturday, December 4th, MDH's network team identified a server that was not working properly. The network team immediately launched an investigation to determine the cause of the technical issues. Through routine troubleshooting, they identified activities that they felt warranted escalation to the internal MDH IT Security team. Shortly after that, the MDH network team and cybersecurity team alerted the MDH Chief Information Security Officer (CISO) that they suspected a ransomware attack.

I was notified shortly thereafter and activated the State's cybersecurity incident response plan through the Maryland Security Operations Center (SOC). This action immediately triggered a notification to the State's Cyber-Response Team, including the Maryland Department of Information Technology, the Maryland Department of Emergency Management, Maryland State Police, the Governor's office of homeland security, and the Maryland National Guard. Additionally, I notified both the Federal Bureau of Investigation and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency. These notifications are part of our standard response and playbook for cybersecurity incidents.

Additionally, I activated the State's cybersecurity insurance policy through the State Treasurer's office, bringing external forensic resources and advisory resources to help ensure that we are handling the incident in the best possible way. The companies and personnel provided by the insurance policy are widely regarded as the best in the industry, and we appreciate the ability to involve them through the Treasurer's insurance policy.

These actions brought together all the resources needed to facilitate a comprehensive investigation and secure recovery.

At my direction and in accordance with our incident response playbook, MDH took immediate containment action by isolating their sites on the network from one another, external parties, the Internet, and other State networks.

As a result of this containment approach, some services were rendered unavailable – the data updates to the COVID dashboard being the most visible. Again, I want to be clear: this was our decision and a deliberate one, and it was the cautious and responsible thing to do for threat isolation and mitigation.

I want to reiterate that this was a ransomware attack on MDH systems.

Ransomware is a type of malware that prevents authorized users from accessing data and systems until an extortion payment is made. Some cybercriminals also use what is known as the "Triple-Threat," consisting of malware, data theft, and denial of service attacks as part of their extortion ploy. While an unsuccessful distributed denial-of-service attack did follow the ransomware event, we have no evidence to suggest that it originated with the same adversary. In addition, we have not identified, to this point in our ongoing investigation, evidence of unauthorized access to or acquisition of data.

As many of you know, and as the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS) have all indicated, cybercriminals are actively targeting the healthcare and public health sector. Furthermore, cybercriminals have taken advantage of the pandemic crisis, and as one report by the cloud security firm Bitglass noted, *"Cyberattacks against U.S. healthcare entities rose by over 55% in 2020 compared with the previous year*" and "*these attacks also increased in sophistication and scale.*" Unlike many organizations, which take days or weeks to contain security incidents, MDH isolated and contained its systems within several hours of first detecting the incident.

We are continuing our thorough forensic investigation, and there is no evidence at this time that this incident resulted in unauthorized access to, or acquisition of, any data.

Since the discovery of this attack, our teams and partners have been working tirelessly and continuously to contain and investigate the incident, as well as safely restore full functionality to MDH's network systems. In cybersecurity incidents, there can be pressure to reconstitute services quickly and sometimes too quickly. All too common are stories of organizations that had to restart recovery efforts because of this, sometimes more than once. While this process may seem slow, we are recovering with deliberate action to minimize the likelihood of reinfection.

I cannot stress how important this point is - in order to protect the state's network and the citizens of the state of Maryland, we are proceeding carefully, methodically, and as expeditiously as possible, to restore data and services. In addition, the State of Maryland

will continue adapting and hardening our IT infrastructure and defenses, in order to help protect the information that is in our care. We take this responsibility very seriously.

Deputy Secretary Lance Schine

My name is Lance Schine, and I am the Deputy Secretary of the Maryland Department of Information Technology, or DoIT, as well as the state's CTO. I have been in this position since Feb. 2017, and prior to that I served as the:

- Chief Technology Officer for the Maryland Department of Human Services;
- the Deputy Chief Technology Officer of Washington, DC; and
- the Chief Information Officer for the Washington, DC Department of Transportation.

From the moment this incident was detected, our actions have been guided by the principle of protecting the systems and data in our care, as well as the health and safety of Marylanders. Throughout this process, we have prioritized restoring health and safety functions, and have made good progress on bringing systems back online as safely and quickly as possible.

As Chip indicated, MDH, together with DoIT and a network of internal and external partners, has been working around-the-clock to contain and isolate the threat and safely restore system functionality and delivery of services – many of which have already been restored. Fortunately, because of the State's aggressive cybersecurity strategy, and the use of MD THINK and other cloud-based services, the incident did not affect many of the Department's core functions.

For those who may not know what MD THINK is, it is Maryland's Total Human-services Integrated Network. An innovative, cloud-based platform — allowing multiple health and human services state agencies to share and manage data in one encrypted secure system. This integrated platform gives us the opportunity to provide citizens with more comprehensive and coordinated assistance across our agencies in order to achieve Maryland's citizen-centric vision.

While being clear not to minimize this attack, we also know this could be much worse. In fact, many/ of MDH's core functions were unaffected, including:

- Medicaid eligibility and enrollment;
- COVID vaccination and hospitalization figures; and,
- Additional core department functions.

With respect to impacted functions and COVID-19 data and services:

- MDH resumed reporting COVID-19 vaccination and hospitalization data on Dec 7 and Dec 8, respectively;
- Topline COVID-19 surveillance reporting suspended temporarily began again on Dec 20; and
- MDH resumed reporting for COVID-19 confirmed and probable deaths and death information by jurisdiction on Dec 28.

- The COVID data that you see on the website is a result of a lot of complicated processes, systems, and data coming together. When the incident occured and systems were taken down, we needed to identify the safest way to make the COVID data available as quickly as we could, all while making sure the systems were secure and could continue to be investigated. In order to ensure that this data being used to make critical decisions was accurate, secure, and trustworthy, we needed to be very deliberate in validating all processes involved in making the data available, and could not rush to release this information until we were certain it was ready - which is what we did.

Additionally:

- MDH restored the ability of Maryland's Electronic Vital Records Registration System (EVRS) to issue death certificates on Dec 18; and
- MDH restored the Electronic Data Interchange Transaction Processing System (EDITPS) connectivity on Dec 15, enabling the resumption of payments to our Medicaid providers.

Again, the incident investigation and response are ongoing and involve multiple agencies and partners – including state and federal law enforcement with respect to criminal liability.

Deputy Secretary Atif Chaudhry

My name is Atif Chaudhry, and I am the MDH Deputy Secretary for Operations. My role today is to discuss MDH's efforts that are ensuring business and service continuity in the aftermath of the attack.

MDH and DoIT are working closely to address this incident and have implemented the FEMA Incident Command System, or ICS, which provides a flexible mechanism for coordinated and collaborative incident management that includes the sharing of resources.

Under this ICS system, we have formed a Unified Command Structure to address this incident, which permits MDH and DoIT to jointly collaborate to manage and address all matters. DoIT provides the technical expertise and is taking the lead on network security and IT system recovery efforts. MDH is focusing on business continuity and ensuring the Department is able to continue to provide services that are in-line with our mission to promote and improve the health and safety of all Marylanders.

MDH business units have existing Continuity of Operations Plans – known as COOP Plans – which provide a methodology and plan for programs to continue performing essential functions in the event of an emergency or interruption of services, such as this attack.

MDH's COOP Plans were initiated and implemented in the hours immediately after the incident was first detected on Saturday, December 4th.

It’s important to note that all of these COOP Plans have been implemented, executed, and modified accordingly, when necessary. That last point is critical: an effective COOP Plan and recovery effort cannot be static, it must be adjusted to meet the particulars of the incident you’re facing.

Immediately following the attack, and in accordance with the Department’s COOP plan, MDH started assessing the business functions that were impacted and began to prioritize them. In this instance, we are using a tiered system that is focused on mission critical and life-safety business functions. This prioritization of the Department’s affected functions has led to the development of a Critical Path for recovery and bringing systems back online.

MDH also immediately began implementing modified workflows for business processes across the Department in order to continue to provide services in accordance with existing and modified COOP Plans, focusing on mission critical and life-safety services.

These solutions include Maryland’s previous – and prescient – decision to migrate to Google Workspaces. This has permitted access to a full suite of online tools unaffected by the incident, and allows MDH to continue to collaborate and save and share critical files.

MDH is continually reviewing business functions and processes, and is working to implement modified workflows to ensure continued operations and functionality for the Department.

MDH has also set up hoteling space for MDH employees to be able to do their work on clean equipment in a safe environment.

We have also ordered additional equipment to implement the Department’s COOP Plans and modified business processes. This includes ordering 2,400 laptops, with an additional 3,000 ordered this week. Additionally, MDH also ordered mifi devices, printers, and wireless access points to ensure employees have the equipment to do their jobs and continue to provide services to the citizens of Maryland.

Without a doubt, one of the Department’s mission-critical functions is the State’s ongoing COVID-19 response, and on that aspect we have remained fully operational throughout this incident.

MDH has also ensured that the Department's Healthcare System has remained operational throughout this incident while maintaining standards of care.

We are also working with cybersecurity and systems specialists to support our efforts, and these independent teams have been working alongside us since the earliest days of the response.

I want to thank you for your time today, and look forward to answering any questions you may have. I will now turn it over to Secretary Schrader.

Secretary Dennis R. Schrader

I also want to acknowledge the tremendous work that Chip and Lance and the DoIT and MDH assessment and business operation restoration teams have been doing since early December. Their teams have been working incredibly hard on behalf of Marylanders to assess and get our business processes back online – including over the holidays – and we owe all of them a debt of gratitude.

Now that you have a better understanding of the details of the attack, I want to briefly discuss the evolution of MDH's information technology capabilities over the past six years. Before I do, however, I'm sure that you share my outrage that this act was an attack on all Marylanders in the middle of a pandemic. If we had not made investments during the past six years, this direct hit could have been much worse.

IT EVOLUTION

In 2016, MDH information technology and security lines of authority were blurry, many protective measures were not in place, and who was in charge was not clear. The IT world is dynamic, and new threats emerge constantly that quickly render yesterday's security measures obsolete. Suffice it to say, MDH was well overdue for an IT evolution. This was a major challenge that we deliberately set out to address in 2016. And we have been in a race against time for six years.

In 2016, we estimated that less than 35 percent of the department's actual technology fell under MDH's Chief Technology Officer. Each of MDH's business units had their own independent IT operations. Because of the lack of a more centralized IT oversight process, MDH had nothing in the Major Information Technology Development Project (MITPD) pipeline, and there was no modern disaster recovery site. Since then we have invested $229 million in projects.

In 2017, it was clear that centralized leadership and accountability was needed, and a critical first step in this direction was the hiring of the Department's first Chief Information Officer (CIO), who was empowered to lead all technology operations and development for MDH. In addition, we developed a more direct relationship with the Chesapeake Regional Information System for our Patients (CRISP), the state's health information exchange that enabled us to build a major public health tool that has become invaluable during the pandemic.

In 2018, we commenced the process to consolidate MDH Hospital IT under MDH's Office of Enterprise Technology (OET) and CIO. We also committed $90 million of Medicaid investments to jumpstart MD THINK. A MITDP was also utilized to begin the process of consolidating data centers, as well as to establish a modern disaster recovery site. In 2018, MDH also established a 10-year, $500 million Medicaid Modular Transformation (MMT) program with the Centers for Medicare and Medicaid Services (CMS).

Progress continued in 2019 with MDH initiating the project to consolidate of several data centers and planning for a modern disaster recovery site. We also began to move the Vital Statistics Administration (VSA) birth and death records to the MDThink platform. Birth records were successfully transitioned and death records, fortunately, were completed in December 2021. In addition, we also migrated Long Term Care Medicaid Eligibility and Enrollment and the Maryland Health Benefit Exchange to MDThink.

In 2020, MDH hired its own Chief Information Security Officer (CISO), as well as a Medicaid Enterprise Systems (MES) Director and further deepened our ties with DoIT through an MOU, which included conducting a cybersecurity survey project. With the onset of COVID in 2020, MDH began preparing to collect and tabulate COVID, vaccination, and other data, which DoIT and CRISP heavily supported.

During this past year, completed the consolidation of data centers at TierPoint and continued to migrate applications to MDTHINK. We established our state-of-the art disaster recovery site in Dallas, and created new MDH policies and procedures pertaining to Data Use, Business Continuity, and Incident Management. We also began our work to implement the Governor's July 2021 Executive Orders, which established a privacy and data officer for each cabinet-level Department.

In conclusion, in six years, information technology and security at MDH has gone from a loose constellation of initiatives and responsibilities into a much more centralized, strategic, and resilient system. The cybersecurity foundation we have built and the modern system we are growing has been instrumental in helping us to absorb this attack. There remains important work to be done for sure, as the December 4th attack reminded us. Our ability to identify and mitigate this attack in a few hours, as well as the pace of the ongoing restoration effort, speaks to this evolution.

I thank the committees for your time. We are now happy to take your questions.